ECE 4823-8803

Hardware-Oriented Security and Trust

Final Exam

April 28, 2022

*This test is open book for the required as well as the optional textbooks. This test is also open note. Calculators are permitted but no programs may be used. Open notes include electronic notes with any handwritten or typed information you may have added. For electronic notes, all wireless connectivity must be turned off, and no cell phone is allowed; in other words, no connection to any information source outside of the open books, notes and items downloaded from the course website is allowed during the exam. Open notes also include all course assignments (homeworks or labs) as well as solutions (including both your solution as well as official solutions posted on the course website or passed out for previous exams). All aspects of the Georgia Tech Honor Code apply. Please follow the instructions precisely. If you need to continue a problem, please use the back of the **previous** page. The meaning of each question should be clear, but please state any assumptions and ask for clarification if necessary.*

You can do it!

Name (Please print)_____

This test will be conducted according to the Georgia Tech Honor Code.
I pledge to neither give nor receive unauthorized assistance on this exam and to abide by all provisions of the Honor Code.

Signed_____

Question	Score	Max
1		**10**
2		**15**
3		**20**
4		**20**
5		**10**
6		**15**
7		**10**
8		**30**
9		**10**
10		**10**
11		**10**
Total		**130 or 160**

1. **(10 pts.) AES and (iii) Encrypt-then-Authenticate.**

Is it possible to implement (iii) encrypt-then-authenticate in Cipher Block Chaining (CBC) mode only given AES and a true random number generator (TRNG) as cryptographic primitives? If so, how? If not, why not?

Please assume that entity authentication has already occurred and the necessary keys have already been exchanged. For example, you can assume that two 128-bit keys, K_1 and K_2, are already provided as an assumption in answering this question.

Please note that if you say it is **not** possible but give no valid reason as to why not, you will receive zero points. Similarly, if you say that it **is** possible but do not explain how with at least one correct intuitive reason, you will receive zero points; in other words, the explanation of how it **is** possible does not need to be exhaustive but only needs to be intuitively correct.

Finally, please limit your answer to approximately 10 sentences

(a) State either (i) “it is possible” or (ii) “it is **not** possible.” A correct answer here alone will earn zero points but will allow the answer below to earn full credit. An incorrect answer here will lose all points for this problem regardless of what is written below for part (b).

(b) Explain at least one valid reason for your answer to part (a) above using 10 sentences or less where drawings and math equations do not count towards this limit of 10 sentences.

2. (15 pts.) Message Authentication Codes.

Suppose that a sender and receiver agree to only support messages of length 3*n* or 10*n*. In other words, sender and receiver agree in advance that $\mathrm{Vrfy}_k(m,t) = 1$ **iff (**$t \stackrel{?}{=} \mathrm{Mac}_k(m)$**) and either (**$|m| = 3$ blocks**) or (**$|m| = 10$ blocks**)**. Is it possible for an adversary to forge a valid tag on a new message?

Please assume that the adversary has access to a MAC oracle which only outputs tags for messages of length 3*n* or 10*n*; i.e., messages of any other length are not provided with a tag. Also assume that *n* is a fixed value for the block size and cannot be changed (e.g., *n* = 128 bits). Finally, as defined in the adaptive chosen message attack, the adversary may choose any message desired; only one message of length 3*n* or 10*n* with a valid tag suffices to answer this question, but keep in mind that the message with a valid tag is only considered to be forged if the exact message was never itself submitted to the MAC oracle.

A correct "yes" or "no" answer without valid reasons for the answer will earn zero points. Only one valid reason is needed, but multiple reasons or statements with some false statements will lose points for the false statements (or false reasons) given even if other valid reasons are given. Please limit your answer to 10 sentences or less (math equations do not count towards this limit), and feel free to circle the part you want graded, cross out parts you do not want graded, or otherwise clearly indicate what is the answer you want considered for a grade.

3. **(20 pts.) The Needham-Schroeder Protocol.**

Consider the Needham-Schroeder protocol, corrected by Lowe, where A is an identifier for Alice, B is an identifier for Bob, $E_A()$ is encryption with a symmetric key held by Alice, $E_B()$ is encryption with a symmetric key held by Bob, K is a symmetric key, and both N_A and N_B are nonces:

1) Alice to Trent: A, B, N_A
2) Trent to Alice: $E_A(N_A, B, K, E_B(K, A))$
3) Alice to Bob: $E_B(K, A)$
4) Bob to Alice: $E_K(B, N_B)$
5) Alice to Bob: $E_K(N_B - 1)$

Now instead consider the asymmetric key version of the same protocol (corrected by Lowe):

1) Alice to Trent: A, B
2) Trent to Alice: $E_{Tpriv}(B_{pub}, B)$
3) Alice to Bob: $E_{Bpub}(N_A, A)$
4) Bob to Trent: B, A
5) Trent to Bob: $E_{Tpriv}(A_{pub}, A)$
6) Bob to Alice: $E_{Apub}(B, N_A, N_B)$
7) Alice to Bob: $E_{Bpub}(N_B)$

Now you are going to be asked to argue in favor of each of these versions. If you believe any assumptions are needed for your answer, please clearly state any such assumptions.

(a) (10 pts.) For your new scooter company of 2000 scooters operating in the City of Atlanta, argue in favor of using the **symmetric** key version of the Needham-Schroeder protocol, corrected by Lowe. For full credit, you only need to give one valid reason why the symmetric key version of the protocol is superior to the asymmetric key version. Please limit your answer to 10 sentences or less.

(b) (10 pts.) For your new scooter company of 2000 scooters operating in the City of Atlanta, argue in favor of using the **asymmetric** key version of the Needham-Schroeder protocol, corrected by Lowe. For full credit, you only need to give one valid reason why the asymmetric key version of the protocol is superior to the symmetric key version. Please limit your answer to 10 sentences or less.

4. **(20 pts.) Arbiter and RO PUFs.**

Consider an Arbiter PUF and a Ring Oscillator (RO) PUF.

(a) (10 pts.) Given an input size of *n*, can an RO PUF generate an exponential number of response bits under ideal conditions (i.e., excluding consideration of model building or machine learning)? A correct "yes" or "no" answer without any valid reason given will earn zero points. Please limit your answer to at most 10 sentences.

(b) (10 pts.) Given an input size of *n*, can an Arbiter PUF generate an exponential number of response bits under ideal conditions (i.e., excluding consideration of model building or machine learning)? A correct "yes" or "no" answer without any valid reason given will earn zero points. Please limit your answer to at most 10 sentences.

5. **(10 pts.) Key Expansion in AES.**

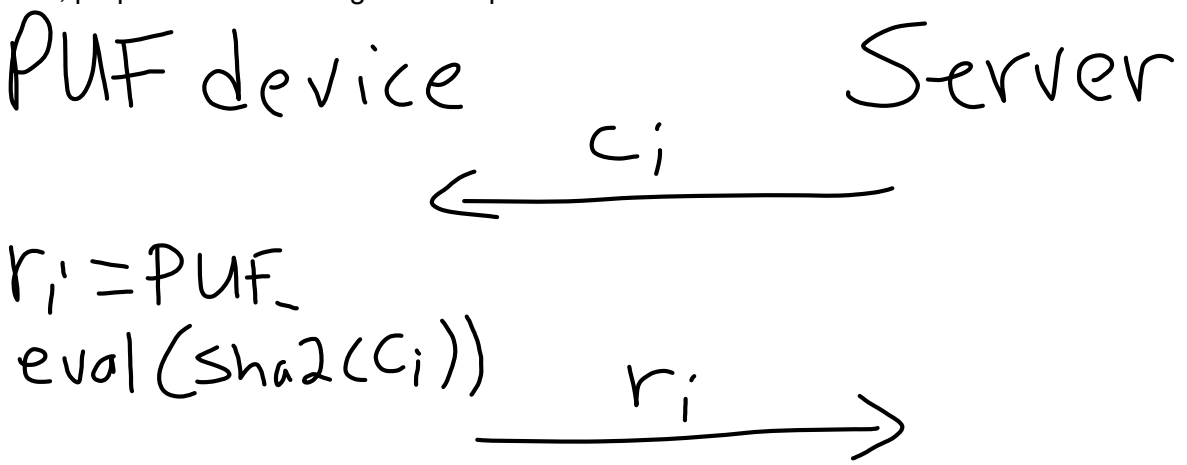
AES with a 128-bit key carries out expansion using the following pseudocode:

Input: key of size 16 bytes denoted $k_0, k_1, \ldots, k_{15}$
Output: key of size 176 bytes denoted $w_0, w_1, \ldots, w_{175}$
Let there be 10 variables
Variables:
rc1 = 0x01000000, rc2 = 0x02000000, rc3 = 0x04000000, rc4 = 0x08000000,
rc5 = 0x10000000, rc6 = 0x20000000, rc7 = 0x40000000, rc8 = 0x80000000,
rc9 = 0x1B000000, rc10 = 0x36000000
Functions:
SubWord: 4 bytes $\rightarrow$ 4 bytes
$a_0, a_1, a_2, a_3 \mapsto \text{Sbox}(a_0), \text{Sbox}(a_1), \text{Sbox}(a_2), \text{Sbox}(a_3)$
RotWord: 4 bytes 4 bytes
$a_0, a_1, a_2, a_3 \mapsto a_1, a_2, a_3, a_0$
KeyExpansion: 16 bytes $\rightarrow$ 176 bytes
for (i=0 to 3) {$w_{4i} = k_{4i}$; $w_{4i+1} = k_{4i+1}$; $w_{4i+2} = k_{4i+2}$; $w_{4i+3} = k_{4i+3}$;}
for (i=4 to 43) { if (i is divisible by 4) {
temp = SubWord(RotWord(w_{4i-4} , w_{4i-3} ,w_{4i-2}, w_{4i-1})) $\oplus$ ($rc_{(i/4)-3}$, $rc_{(i/4)-2}$, $rc_{(i/4)-1}$, $rc_{(i/4)}$);
} else {
temp = (w_{4i-4} , w_{4i-3} ,w_{4i-2}, w_{4i-1});
}
(w_{4i} , w_{4i+1} ,w_{4i+2}, w_{4i+3}) = temp $\oplus$ (w_{4i-16} , w_{4i-15} ,w_{4i-14}, w_{4i-13});
}

What function or role does RotWord fulfill in key expansion in AES? Please describe a cryptographic property that is served or advanced by RotWord. For full credit, your answer must contain an intuitive explanation beyond just providing a technical name of a cryptographic property. For example, if the answer to this question were "Man-in-the-Middle" (which is obviously **not** the answer to this question!), an answer giving the buzzword "Man-in-the-Middle" with no description of how the MitM attack is realized would earn at most half of the points for this problem. Please explain your answer clearly with an intuitive explanation in at most 10 sentences.

6. **(15 pts.) Hashing PUF Challenges.**

Your company purchases a PUF which claims to be a strong PUF yet contains legal language in the purchase agreement that says the PUF company is not liable if it turns out based on later information that the PUF is in fact weak. Therefore, an engineer on your team, say the engineer's name is Alex, proposes the following three steps:



Please assume that the rest of the protocol not shown (e.g., use of a database of challenge-response pairs) works correctly. The basic idea shown above is to hide the challenge by use of SHA2. Alex is convinced that this idea will prevent model building attacks. Do you agree or disagree with Alex and why? Please note that this problem will be graded based on the reasons given for agreeing or disagreeing; only one solid reason which is a correct reason is needed for full credit, but a mix including incorrect reasons will lose points. In cases where you want some of what you write to be disregarded or ignored, please clearly indicate which text you want to be graded as your final answer.

(a) State either (i) "I agree with Alex" or (ii) "I disagree with Alex." A correct answer here alone will earn zero points but will allow the answer below to earn full credit. An incorrect answer here will lose all points for this problem regardless of what is written below for part (b).

(b) Explain at least one valid reason for your answer to part (a) above using 10 sentences or less.

7. **(10 pts.) Diffie-Hellman Key Exchange.**

Consider the case of Diffie-Hellman Key Exchange using $\alpha = 6$ as a generator for Z_{13}^*. Below are a list of possible secrets x, y and associated modulus answers including the final shared key K. Are any of the answers below incorrect? If your answer is "yes," you must correctly indicate at least one answer which is incorrect. If your answer is "no," then obviously there is no need to say anything additional. Please note that to receive full credit for this problem you must not have any incorrect answers to this question; for example, if you say "yes" and indicate two answers are incorrect where in fact only one of the answers is incorrect, you will receive half credit.

x, y	α^x	α^y	$(\alpha^x) \bmod p$	$(\alpha^y) \bmod p$	K
2,3	36	216	10	8	12
2,4	36	1296	10	9	3
2,5	36	7776	10	2	4
2,7	36	279936	10	7	10
2,8	36	1679616	10	3	9
2,10	36	60466176	10	4	3
3,4	216	1296	8	9	1
3,5	216	7776	8	2	8
3,6	216	46656	8	12	12
3,7	216	279936	8	7	5
3,11	216	362797056	8	11	5
4,6	1296	46656	9	12	1
4,7	1296	279936	9	7	9
4,8	1296	1679616	9	3	3
4,9	1296	10077696	9	5	1
4,11	1296	362797056	9	11	3
5,6	7776	46656	2	12	12
5,7	7776	279936	2	7	11
5,8	7776	1679616	2	3	9
7,8	279936	1679616	7	3	3
7,9	279936	10077696	7	5	8
7,11	279936	362797056	7	11	2
8,10	1679616	60466176	3	4	3
9,11	10077696	362797056	5	11	8

.

8. **(30 pts.) Reverse Fuzzy Extractor.**

Consider the Reverse Fuzzy Extractor protocol as shown:

Protocol 3: Reverse Fuzzy Extractor

Prover (token ht_i with ID_i)		Verifier (server)
$\text{PUF}_i \rightarrow r'_i$ (PUF produces r'_i)	A. Van Herrewege, S. Katzenbeisser, R. Maes, R. Peeters, A.-R. Sadeghi, I. Verbauwhede, and C. Wachsmann, "Reverse Fuzzy Extractors: Enabling Lightweight Mutual Authentication for PUF-enabled RFIDs", *Vol. 7397 of Lecture Notes in Computer Science*, 2012, pp. 374-389	
$\text{hd}_i = r'_i \bullet \text{H}^{\text{T}}$ (Helper data hd_i computed)		
$n_1 \leftarrow TRNG()$ (Nonce n_1 generated)	$ID_i, \text{hd}_i, n_1 \rightarrow$	$\text{DB}[ID_i] \rightarrow r_i$ (Server looks up r_i) $r''_i = \text{Rep}(r_i, \text{hd}_i)$ (And error corrects it to r''_i) $n_2 \leftarrow TRNG()$ (Nonce n_2 generated) $m_1 = h(ID_i, \text{hd}_i, r''_i, n_1, n_2)$ (Unkeyed hash of protocol vals)
$h(ID_i, \text{hd}_i, r'_i, n_1, n_2) \stackrel{?}{=} m_1$ (Accept if match, else abort)	$\leftarrow m_1, n_2$	
$m_2 = h(ID_i, r'_i, n_2)$ (Unkeyed hash of protocol vals)	$m_2 \rightarrow$	$h(ID_i, r''_i, n_2) \stackrel{?}{=} m_2$ (Accept if match, else abort)

Authentication

(a) (5 pts.) If authentication fails, what is one possible explanation for the failure?

(b) (5 pts.) If authentication fails, what is a second possible explanation? For credit you must provide an answer that is clearly distinct and unique (no overlap) as compared to the answer provided on the previous page for part (a).

(c) (20 pts.) The Reverse Fuzzy Extractor protocol as shown uses an unkeyed hash such as SHA2. However, a keyed hash such as a MAC could be used in place of the unkeyed hash. Would the use of a keyed hash such as a MAC be beneficial in the Reverse Fuzzy Extractor protocol over the use of an unkeyed hash? If the use of a keyed hash would be beneficial, what would be at least on specific benefit? If there is no benefit, why is it that an unkeyed hash provides equal protection as compared to use of a keyed hash in the Reverse Fuzzy Extractor protocol? Please limit your answer to 10 sentences.

9. **[ECE 8803 only] (10 pts.) HELP and NIST.**

Suppose a particular implementation of the HELP PUF had enough sample size (approximately 10^{15} samples) to attempt all of the NIST tests for randomness. Suppose further that the overall conclusion is that the HELP PUF tested passes all of the tests. Would this successful result passing the NIST tests certify that the HELP PUF tested cannot be machine learned? Stated another way, does successfully passing the NIST tests guarantee that the specific HELP PUF tested cannot have a model built which would predict challenge-response pairs?

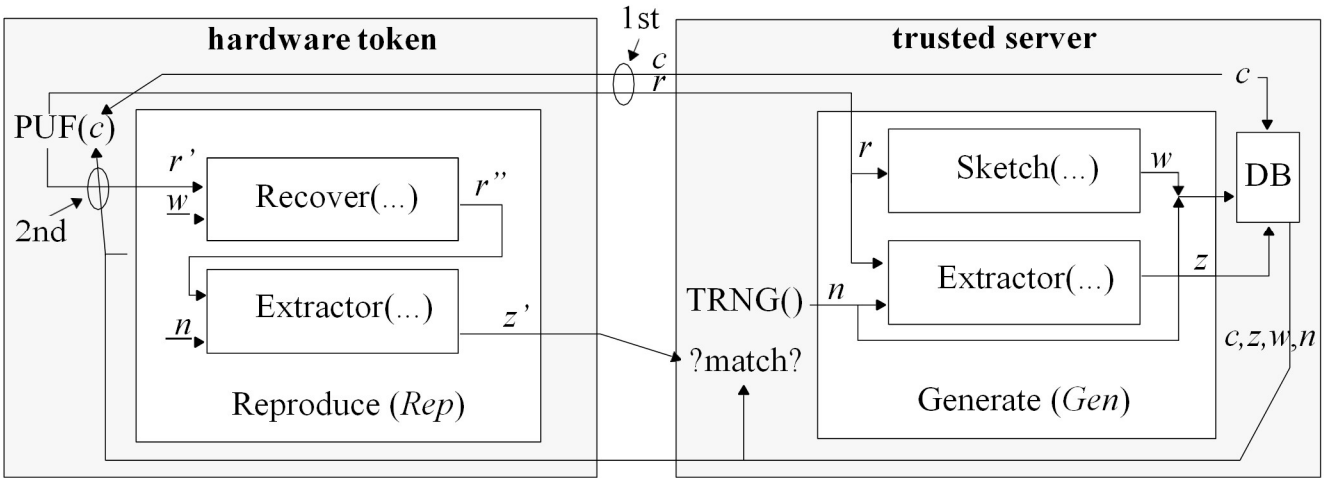
A correct "yes" or "no" answer without any valid reason given will earn zero points. Please limit your answer to at most 10 sentences.

10. **[ECE 8803 only] (10 pts.)**

When a file is compressed, what happens to the overall entropy or randomness in the file? For example, consider a file of 2048 bytes of ASCII where due to the language statistics each byte of ASCII text actually only contains three bits of entropy. In this case the entropy total would be $2048*2^3 = 2^{11}*2^3 = 2^{14}$. Now further suppose that after compression the result is 512 bytes. Has the overall entropy or randomness in this resulting file of size 512 bytes increased higher than 2^{14}?

Actually there are three answers possible for this question in the context of this specific example: (i) the overall entropy has increased higher than 2^{14}, (ii) the overall entropy remains equal to 2^{14}, or (iii) the overall entropy is now reduced below 2^{14}. Indicating the correct answer (i), (ii) or (iii) with no correct reason for the answer will earn zero points. For full credit, your answer must contain at least one valid reason and no invalid reasons. Please limit your answer to 10 sentences or less.

11. **[ECE 8803 only] (10 pts.) Helper Data and Fuzzy Extraction.**



Shown above is the fuzzy extractor. The helper data *w* is sent in the clear over a communication channel which may be eavesdropped. Do repeated (e.g., 2nd and 3rd) transmissions of helper data *w* over time **increase** the possibility of information leakage (i.e., over and beyond any information leakage that occurred the first time)? Please answer in two steps as indicated below.

(a) Please state one of the following options: (i) "each repeated transmission of helper data *w* over time increases the possibility of information leakage" or (ii) "each repeated transmission of helper data *w* over time does not increase the possibility of information leakage." NOTE: you may want to answer part (b) below first.

(b) Why does – or does not – each repeated transmission of helper data *w* over time increase the possibility of information leakage? Please note that an incorrect answer to part (a) above loses all of the points for this problem. A correct answer to part (a) requires also at least one valid reason here in part (b) to earn points. A mix of correct and incorrect reasons or statements will lose some points for the incorrect reasons/statements. Please limit your answer to 10 sentences or less.

THIS IS THE LAST PAGE OF THE EXAM!